HACKING 101

This article is the second in a series of articles that address the oft-asked question, "How do I become a hacker?"

Targeting Theory

By StankDawg *(StankDawg@hotmail.com)*

So you want to "hack" a system, eh? But what exactly does that mean? Where exactly does one start to hack into a system? "Teach me how to hack!" Well, this article is fundamental in understanding how to target and attack a system. This article is meant for security professionals and hobbyists to understand the concepts of hacking. This article is also meant for hackers who want to understand the same concept. Even advanced hackers do not fully understand or appreciate the fundamental steps that go on inside the hacker mind. This is a crucial lesson in developing and understanding the mindset of a hacker.

This is a theory topic, meaning it is about understanding a theoretical concept about hacking. This is not a specific detailed account of how to apply a specific exploit or attack on a system. This is on a much higher level. Understanding fundamental concepts such as "targeting theory" will take you much further than a specific one time trick or "how-to" lesson. This is a critical concept to learn and use for all hacking application.

When I say "targeting theory" I am referring to the research, analysis, evaluation, and determination of where the most appropriate place to attack a system is. More simply put: What method and location of attack is going to be the most likely place of gaining access? For "play" hacking, you may simply stumble across a site or a server and just look at what is presented to you. You poke around, perhaps finding some loopholes or logic bugs that allow you some extra access. This is incredibly fun, don't get me wrong, but if you actually want to "root" the system, you need a more analytical approach.

This is when we apply targeting theory. You have a server that you have decided to access (preferably your own for testing purposes, or one that you have permission to test) you apply the techniques of "footprinting" a system to find out everything that you can about that system. Find out the information about how it allows access (internet, dial-up, physical only, etc…). Discover what operating system it runs. See what applications it runs. If it is connected to the internet, what open ports does it have? Basically, any bit of information you can find will help give you an overall understand of the system. Only with this can you begin proper analysis.

Depending on what you find in the results of your footprint analysis, you must then extract the most useful information from the results. Make a list or a chart of the information that you feel is most appropriate. To give a specific example, I would suggest four separate columns of the following: Network, Ports, OS, and, Applications. Take a look at a very small example list that could be using data garnered from footprinting a system. The first article in the ***HACKING 101*** series was about how to footprint a system and was originally published in Binary Revolution magazine issue 1.1 which is available at ***www.binrev.com*** for online ordering.

Network	Ports	OS	Applications
192.168.0.1	21 / FTP	Windows NT 4.0	IIS 3.0
192.168.0.1	80 / HTTP	Windows NT 4.0	IIS 3.0
192.168.0.2	21 / FTP	Linux (Redhat 7.2)	wu-ftpd 2.6.0
192.168.0.2	23 / Telnet	Linux (Redhat 7.2)	??? (unknown)
192.168.0.2	80 / HTTP	Linux (Redhat 7.2)	Apache